ACTA ARITHMETICA
160.1 (2013)

Normal integral bases and tameness conditions for Kummer extensions

by

Ilaria Del Corso and Lorenzo Paolo Rossi (Pisa)

1. Introduction. Let K be a number field and let $\mathcal{O}_K$ be its ring of integers. A finite normal extension L/K with Galois group G has a *normal integral basis* (NIB for short) when $\mathcal{O}_L$, the ring of integers of L, is free of rank one over the group ring $\mathcal{O}_K[G]$. In this case, if $\mathcal{O}_L = \mathcal{O}_K[G]\omega$, we call ω a *generator* of the NIB.

A well known result by Noether says that if L/K has a NIB, then it is a tamely ramified extension. The converse is not true in general and there are several examples of non-existence of a NIB for tamely ramified extensions. Even if we restrict to the class of abelian extensions, the general situation cannot be easily described. On the one hand, by the Hilbert–Speiser Theorem, in the case when the base field K is the field $\mathbb{Q}$ of rational numbers, every tame abelian extension L/K has a NIB. On the other hand, Greither et al. [6] proved that $\mathbb{Q}$ is the only number field satisfying the conclusion of the theorem of Hilbert and Speiser. Namely, for any number field $K \neq \mathbb{Q}$ there exists a prime number p and a tame cyclic extension L/K of degree p without a NIB.

Several authors considered the particular case of Kummer extensions; in the case when the degree is prime, Gómez Ayala gave an explicit criterion [5, Thm. 2.1] for the existence of a NIB. More recently the present authors [3, Thm. 1] proposed a generalization of that result to cyclic extensions of arbitrary degree.

In this paper we consider the general case of tamely ramified Kummer extensions and in Theorem 11 we obtain a criterion for the existence of a NIB which generalizes the previous results. As in the case of cyclic extension, the methods used in the proof of Theorem 11 also allow us to describe explicitly the Steinitz class of a tame Kummer extension, giving an easy criterion for this class to be trivial (Propositions 13 and 29).

2010 *Mathematics Subject Classification*: 11R33, 11S15.
Key words and phrases: Kummer extensions, NIB, tame extensions.

DOI: 10.4064/aa160-1-1

In the second part of the paper we restrict to the particular case of Kummer extensions generated, over $\mathbb{Q}(\zeta_m)$, by mth roots of rational integers.

Section 3.1 is devoted to a detailed study of the ramification in extensions $\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}(\zeta_m)$ with $a \in \mathbb{Z}$; we find necessary and sufficient explicit conditions on a for the tameness of these extensions (see Proposition 24 and Corollary 25).

In Sections 3.2–3.4 we present some results on the existence of integral bases for tame extensions of the kind $\mathbb{Q}(\zeta_m, \sqrt[m]{a_1}, \dots, \sqrt[m]{a_n})/\mathbb{Q}(\zeta_m)$, with $a_i \in \mathbb{Z}$. Firstly, we prove that these extensions always have trivial Steinitz classes, hence an integral basis (see Proposition 29). We also give sufficient conditions for the existence of a normal integral basis for such extensions and an example showing that such conditions are sharp in the general case. This result generalizes the well known result by Kawamoto [10] and a more recent result by Ichimura [8].

2. Main theorem. In this paper $m \geq 2$ will denote a fixed natural number and ζ_m a primitive mth root of unity. Let K be a number field and let $\mathcal{O}_K$ be its ring of integers; we will always assume that $\zeta_m \in K$. Let L be a Kummer extension of K of exponent m, denote by $\mathcal{O}_L$ its ring of integers and let $G := \mathrm{Gal}(L/K)$.

In this section, in Theorem 11, we will give necessary and sufficient conditions for the existence of a normal integral basis for L/K, namely for the existence of an element $\omega \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[G]\omega$. To show equality between these two modules, we will compare their discriminants. We start by introducing the notation and developing the tools to compute them.

A *set of Kummer generators* (or *of integral Kummer generators*, resp.) of L over K is any set of elements $\alpha_1, \dots, \alpha_n \in L$ ($\alpha_1, \dots, \alpha_n \in \mathcal{O}_L$, resp.) such that, setting $m_i := [K(\alpha_i) : K]$, we have

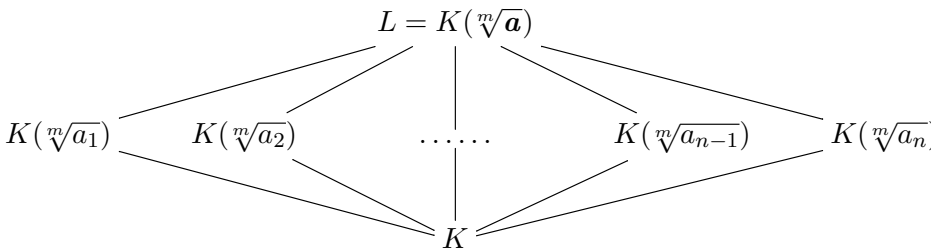
1. $L = K(\alpha_1, \dots, \alpha_n)$;
2. $\alpha_i^{m_i} \in K$ for $i = 1, \dots, n$;
3. $[L : K] = \prod_{i=1}^{n} m_i =: N$.

By Kummer theory it is clear that for any finite Kummer extension, there exists a set of Kummer generators; moreover, if $\alpha_1, \dots, \alpha_n$ is a set of Kummer generators, then there exist $c_1, \dots, c_n \in \mathcal{O}_K$ such that $c_1\alpha_1, \dots, c_n\alpha_n$ is a set of integral Kummer generators. We also remark that the exponent of this kind of extension is the least common multiple of the m_i's, thus we may set $m = \mathrm{lcm}(m_1, \dots, m_n)$.

For $i = 1, \dots, n$, we put $a_i = \alpha_i^m$; since $m_i \mid m$, it is clear that $a_i \in K$ for all i and we use the notation $L = K(\sqrt[m]{\boldsymbol{a}})$, where $\boldsymbol{a} = \{a_1, \dots, a_n\} \in K^n$ and $\sqrt[m]{\boldsymbol{a}} = \{\sqrt[m]{a_1}, \dots, \sqrt[m]{a_n}\}$.

In the following, for simplicity of notation, we will always assume that $\{\alpha_1, \dots, \alpha_n\} = \sqrt[m]{\boldsymbol{a}}$ is a set of integral Kummer generators of L/K, but we note that sometimes it would not be necessary to assume property 3.

With the given notation we have the following diagram:



and

$$G = \mathrm{Gal}(L/K) = \bigoplus_{i=1}^{n} \mathrm{Gal}(K(\alpha_i)/K) \cong \bigoplus_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}.$$

Our first step is to compute, in the case when $L = K(\sqrt[m]{\boldsymbol{a}})/K$ is tame, the discriminant of the extension, $\mathrm{disc}(L/K)$, in terms of $\boldsymbol{a}$.

Let $\mathcal{P} \subset \mathcal{O}_K$ be a prime ideal; we denote by $e_{\mathcal{P}}$ its ramification index in $\mathcal{O}_L$ and, for any ideal $\mathcal{I} \subset \mathcal{O}_K$, by $\mathrm{ord}_{\mathcal{P}}(\mathcal{I})$ the exact power of $\mathcal{P}$ dividing $\mathcal{I}$.

LEMMA 1. *Let $\mathcal{P}$ be a prime ideal of $\mathcal{O}_K$. If $\mathcal{P}$ is tamely ramified in $\mathcal{O}_L$, then*

$$\mathrm{ord}_{\mathcal{P}} \mathrm{disc}(L/K) = N - N/e_{\mathcal{P}}.$$

Proof. This follows easily from the theorem of Dedekind on discriminants. ∎

LEMMA 2 ([3, Lemma 3]). *Let $L = K(\sqrt[m]{a})$ with $a \in \mathcal{O}_K$. Then, for any prime $\mathcal{P} \subseteq \mathcal{O}_K$ tamely ramified in $\mathcal{O}_L$, we have*

$$e_{\mathcal{P}} = m/(\mathrm{ord}_{\mathcal{P}}\, a, m). \ \blacksquare$$

The last lemma can be generalized to any Kummer extension (not necessarily cyclic).

We use the following notation:

$$\mathrm{ord}_{\mathcal{P}}\, \boldsymbol{a} = (\mathrm{ord}_{\mathcal{P}}\, a_1, \dots, \mathrm{ord}_{\mathcal{P}}\, a_n) \in \mathbb{Z}^n,$$
$$(\mathrm{ord}_{\mathcal{P}}\, \boldsymbol{a}, m) = \gcd(\mathrm{ord}_{\mathcal{P}}\, a_1, \dots, \mathrm{ord}_{\mathcal{P}}\, a_n, m),$$

and, for any vector $\boldsymbol{w} = (w_1, \dots, w_n)$ and $\boldsymbol{k} = (k_1, \dots, k_n) \in \mathbb{Z}^n$,

$$\boldsymbol{w}^{\boldsymbol{k}} = w_1^{k_1} \cdots w_n^{k_n}.$$

LEMMA 3. *Let $L = K(\sqrt[m]{\boldsymbol{a}}) = K(\sqrt[m]{a_1}, \dots, \sqrt[m]{a_n})$ with $\boldsymbol{a} \in \mathcal{O}_K^n$. Then, for any prime $\mathcal{P} \subseteq \mathcal{O}_K$ tamely ramified in $\mathcal{O}_L$, we have*

$$e_{\mathcal{P}} = m/(\mathrm{ord}_{\mathcal{P}}\, \boldsymbol{a}, m).$$

Proof. Let $d = (\operatorname{ord}_{\mathcal{P}} \boldsymbol{a}, m)$. Then

$$d = k_1 \operatorname{ord}_{\mathcal{P}} a_1 + \cdots + k_n \operatorname{ord}_{\mathcal{P}} a_n + km$$

for some $k_i, k \in \mathbb{Z}$ (we may also suppose $k_i \geq 0$). Let $a = \boldsymbol{a}^{\boldsymbol{k}} = a_1^{k_1} \cdots a_n^{k_n}$. Then $\operatorname{ord}_{\mathcal{P}} a \equiv d \pmod m$. Thus, by Lemma 2, in the extension $K(\sqrt[m]{a})/K$ we have $e_{\mathcal{P}} = m/d$.

Let $F = K(\sqrt[m]{a})$. We now show that, for $i = 1, \ldots, n$, any prime ideal $\mathcal{Q} \subset \mathcal{O}_F$, $\mathcal{Q} \,|\, \mathcal{P}$, is unramified in $F(\sqrt[m]{a_i})/F$; this can be proved by localization and Abhyankar's Lemma (see for example [14, p. 229]). Let us prove it anyway by a direct computation. As $d \,|\, \operatorname{ord}_{\mathcal{P}} a_i$ we have $\operatorname{ord}_{\mathcal{P}} a_i = jd$; thus $\operatorname{ord}_{\mathcal{Q}} a_i = \operatorname{ord}_{\mathcal{P}} a_i \cdot m/d = mj$. Hence, letting $e_{\mathcal{Q}}$ be the ramification index of $\mathcal{Q}$ in $F(\sqrt[m]{a_i})$, by Lemma 2 we get

$$e_{\mathcal{Q}} = \frac{m}{(\operatorname{ord}_{\mathcal{Q}} a_i, m)} = 1.$$

Thus the primes over $\mathcal{P}$ are unramified in the extension $L/K(\sqrt[m]{a})$, and the ramification index of $\mathcal{P}$ in L/K is $e_{\mathcal{P}} = m/d$. ∎

Corollary 4. *Let $L = K(\sqrt[m]{\boldsymbol{a}})$ with $\boldsymbol{a} \in \mathcal{O}_K^n$ and suppose that L/K is tamely ramified. Then*

$$\operatorname{disc}(L/K) = \prod_{\mathcal{P}} \mathcal{P}^{N - \frac{N}{m}(\operatorname{ord}_{\mathcal{P}} \boldsymbol{a}, m)}.$$

Proof. This follows from Lemmas 1 and 3. ∎

Our next step is to study the discriminant of $\mathcal{O}_K[G]\omega$ for $\omega \in \mathcal{O}_L$. To do this we introduce the Lagrange resolvents.

We know that

$$G = \operatorname{Gal}(L/K) = \bigoplus_i \operatorname{Gal}(K(\alpha_i)/K) \cong \bigoplus_i \mathbb{Z}/m_i\mathbb{Z};$$

now, since the global extension has exponent m, it is convenient to view $\operatorname{Gal}(K(\alpha_i)/K)$ as a subgroup of $\mathbb{Z}/m\mathbb{Z}$, so we choose

$$\mathcal{R}_i = \left\{0, \frac{m}{m_i}, 2\frac{m}{m_i}, \ldots, (m_i - 1)\frac{m}{m_i}\right\}$$

as a set of representatives of $\operatorname{Gal}(K(\alpha_i)/K)$, hence

$$\mathcal{R} = \mathcal{R}_1 \times \cdots \times \mathcal{R}_n$$

is a set of representatives of G. We also define

$$\hat{\mathcal{R}}_i = \{0, 1, \ldots, m_i - 1\} \quad \text{and} \quad \hat{\mathcal{R}} = \hat{\mathcal{R}}_1 \times \cdots \times \hat{\mathcal{R}}_n;$$

we have

$$N = |G| = |\mathcal{R}| = |\hat{\mathcal{R}}|.$$

For $i = 1, \ldots, n$ we define σ_i^{m/m_i} to be the generator of $G_i = \operatorname{Gal}(K(\alpha_i)/K)$ sending α_i to $\zeta_m^{m/m_i}\alpha_i$ (we note that $\sigma_i : \alpha_i \mapsto \zeta_m \alpha_i$ is not a well defined map

unless $m = m_i$, but we will always use powers of σ_i with exponent a multiple of m/m_i; these give well-defined homomorphisms). Let χ_i be the generator of $\hat{G}_i$ (the group of characters of G_i) such that $\chi_i(\sigma_i^{m/m_i}) = \zeta_{m_i} := \zeta_m^{m/m_i}$. We can extend σ_i^{m/m_i} to L setting $\sigma_i^{m/m_i}(\alpha_j) = \alpha_j$ if $i \neq j$ and we can also extend χ_i to $G = \mathrm{Gal}(L/K) = \bigoplus_i G_i$ setting $\chi_i(\sigma_j^{m/m_j}) = 1$ if $i \neq j$. Now we define $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_n)$ and $\boldsymbol{\chi} = (\chi_1, \dots, \chi_n)$; for $\boldsymbol{l} \in \mathcal{R}$ we set

$$\boldsymbol{\sigma}^{\boldsymbol{l}} = \sigma_1^{l_1} \circ \cdots \circ \sigma_n^{l_n} \in G$$

and for $\boldsymbol{r} \in \hat{\mathcal{R}}$ we set

$$\boldsymbol{\chi}^{\boldsymbol{r}} = \chi_1^{r_1} \cdots \chi_n^{r_n} \in \hat{G},$$

the group of characters of G. It is clear that, since G and $\hat{G}$ are abelian groups, we have $G = \{\boldsymbol{\sigma}^{\boldsymbol{l}}\}_{\boldsymbol{l} \in \mathcal{R}}$ and $\hat{G} = \{\boldsymbol{\chi}^{\boldsymbol{r}}\}_{\boldsymbol{r} \in \hat{\mathcal{R}}}$.

For $\boldsymbol{l} \in \mathcal{R}$ and $\boldsymbol{r} \in \hat{\mathcal{R}}$ we define

$$\boldsymbol{l} \cdot \boldsymbol{r} = \sum_{i=1}^{n} l_i r_i;$$

moreover, for $\omega \in \mathcal{O}_L$ and $\boldsymbol{r} \in \hat{\mathcal{R}}$ we recall that the *Lagrange resolvent* is

$$\begin{aligned}\omega_{\boldsymbol{r}} = \langle \omega, \boldsymbol{\chi}^{\boldsymbol{r}} \rangle &= \sum_{\sigma \in G} \sigma(\omega) \boldsymbol{\chi}^{\boldsymbol{r}}(\sigma^{-1}) = \sum_{\sigma \in G} \sigma(\omega) \overline{\boldsymbol{\chi}^{\boldsymbol{r}}(\sigma)} \\ &= \sum_{\boldsymbol{l} \in \mathcal{R}} \boldsymbol{\sigma}^{\boldsymbol{l}}(\omega) \overline{\boldsymbol{\chi}^{\boldsymbol{r}}(\boldsymbol{\sigma}^{\boldsymbol{l}})} = \sum_{\boldsymbol{l} \in \mathcal{R}} \boldsymbol{\sigma}^{\boldsymbol{l}}(\omega) \zeta_m^{-\boldsymbol{l} \cdot \boldsymbol{r}}.\end{aligned}$$

LEMMA 5 ([4, (1.3), p. 385]). *Let $\omega \in \mathcal{O}_L$ be such that the conjugates $\{\boldsymbol{\sigma}^{\boldsymbol{l}}(\omega)\}_{\boldsymbol{l} \in \mathcal{R}}$ are linearly independent over K. Then*

$$\mathrm{disc}_{L/K}(\mathcal{O}_K[G]\omega) = \prod_{\boldsymbol{r} \in \hat{\mathcal{R}}} \omega_{\boldsymbol{r}}^2 \mathcal{O}_K. \ \blacksquare$$

Denoting by $[x]$ the largest integer $\leq x$, for any $\boldsymbol{r} \in \mathbb{Z}^n$ we define the *$\boldsymbol{r}$-ideal associated* to $\boldsymbol{a} \in \mathcal{O}_K^n$ to be the ideal

$$\mathcal{B}_{\boldsymbol{r}} = \prod_{\mathcal{P} \subset \mathcal{O}_K} \mathcal{P}^{[\sum r_i \, \mathrm{ord}_{\mathcal{P}} \, a_i / m]} = \prod_{\mathcal{P} \subset \mathcal{O}_K} \mathcal{P}^{[\boldsymbol{r} \cdot \mathrm{ord}_{\mathcal{P}} \, \boldsymbol{a} / m]},$$

that is, the smallest ideal $\mathcal{I} \subset \mathcal{O}_K$ such that $\boldsymbol{a}^{\boldsymbol{r}} \mathcal{I}^{-m}$ is an integral ideal in $\mathcal{O}_K$.

REMARK 6. Let $\boldsymbol{r}' = \boldsymbol{r} + (k_1 m_1, \dots, k_n m_n)$. Then it is easy to see that

$$\mathcal{B}_{\boldsymbol{r}'} = \prod_{i=1}^{n} (\alpha_i^{m_i})^{k_i} \cdot \mathcal{B}_{\boldsymbol{r}}.$$

LEMMA 7. *Let m, m_i and N as above. For $\boldsymbol{l} \in \mathcal{R}$ we have*

$$2\sum_{\boldsymbol{r}\in\hat{\mathcal{R}}}\left[\frac{\boldsymbol{l}\cdot\boldsymbol{r}}{m}\right] = \frac{N}{m}\big(l_1(m_1-1)+\cdots+l_n(m_n-1)\big) - N + \frac{N}{m}(\boldsymbol{l},m).$$

Proof. Denoting by $\{x\}$ the fractional part of x, i.e. $\{x\} = x - [x]$, we have

$$2\sum_{\boldsymbol{r}\in\hat{\mathcal{R}}}\left[\frac{\boldsymbol{l}\cdot\boldsymbol{r}}{m}\right] = 2\sum_{\boldsymbol{r}\in\hat{\mathcal{R}}}\frac{\boldsymbol{l}\cdot\boldsymbol{r}}{m} - 2\sum_{\boldsymbol{r}\in\hat{\mathcal{R}}}\left\{\frac{\boldsymbol{l}\cdot\boldsymbol{r}}{m}\right\}.$$

Let us evaluate these two sums separately:

$$\begin{aligned}
2\sum_{\boldsymbol{r}\in\hat{\mathcal{R}}}\frac{\boldsymbol{l}\cdot\boldsymbol{r}}{m} &= \frac{2}{m}\Big(l_1\sum_{r} r_1 + \cdots + l_n\sum_{r} r_n\Big)\\
&= \frac{2}{m}\left(l_1\frac{N}{m_1}\frac{m_1(m_1-1)}{2} + \cdots + l_n\frac{N}{m_n}\frac{m_n(m_n-1)}{2}\right)\\
&= \frac{N}{m}\big(l_1(m_1-1)+\cdots+l_n(m_n-1)\big).
\end{aligned}$$

Let $d = (\boldsymbol{l}, m)$; the map

$$\varphi : \bigoplus_i \mathbb{Z}/m_i\mathbb{Z} \to d\mathbb{Z}/m\mathbb{Z}, \qquad \boldsymbol{r} \mapsto [\boldsymbol{r}\cdot\boldsymbol{l}]_m,$$

is a surjective homomorphism ($[\boldsymbol{r}\cdot\boldsymbol{l}]_m$ indicates the class of $\boldsymbol{r}\cdot\boldsymbol{l}$ modulo m). In fact, by definition,

$$d = r_1l_1 + \cdots + r_nl_n + rm$$

for some $r_i, r \in \mathbb{Z}$ (we may also suppose $0 \le r_i \le m_i - 1$, because $\boldsymbol{l} \in \mathcal{R}$); thus there exists $\boldsymbol{r} \in \hat{\mathcal{R}}$ such that $[\boldsymbol{r}\cdot\boldsymbol{l}]_m = d$. Hence the map

$$\tilde{\varphi} : \hat{\mathcal{R}} \to \{0, d/m, 2d/m, \ldots, 1-d/m\}, \qquad \boldsymbol{r} \mapsto \{\boldsymbol{r}\cdot\boldsymbol{l}/m\},$$

is surjective and every value in $\{0, d/m, 2d/m, \ldots, 1-d/m\}$ is taken Nd/m times. Hence, setting $M = m/d$, we obtain

$$2\sum_{\boldsymbol{r}\in\hat{\mathcal{R}}}\left\{\frac{\boldsymbol{l}\cdot\boldsymbol{r}}{m}\right\} = 2\frac{N}{M}\sum_{i=0}^{M-1}\frac{i}{M} = 2\frac{N}{M^2}\frac{M(M-1)}{2} = N - \frac{N}{m}\,d. \quad \blacksquare$$

COROLLARY 8.

$$\prod_{\boldsymbol{r}\in\hat{\mathcal{R}}}\mathcal{B}_{\boldsymbol{r}}^2 = \prod_{\mathcal{P}}\mathcal{P}^{\frac{N}{m}(\operatorname{ord}_{\mathcal{P}} a_1(m_1-1)+\cdots+\operatorname{ord}_{\mathcal{P}} a_n(m_n-1))-N+\frac{N}{m}(\operatorname{ord}_{\mathcal{P}}\boldsymbol{a},m)}.$$

Proof. We note that, since $[K(\alpha_i):K] = m_i$, we have $\alpha_i^{m_i} \in \mathcal{O}_K$, thus $a_i := \alpha_i^m = (\alpha_i^{m_i})^{m/m_i}$ is an m/m_ith power in $\mathcal{O}_K$; hence $\operatorname{ord}_{\mathcal{P}}\boldsymbol{a} \in \mathcal{R}$.

Lemma 7 gives

$$\prod_{\boldsymbol{r}\in\hat{\mathcal{R}}}\mathcal{B}_{\boldsymbol{r}}^2=\prod_{\mathcal{P}}\mathcal{P}^{2\sum_{\boldsymbol{r}}[\boldsymbol{r}\cdot\operatorname{ord}_{\mathcal{P}}\boldsymbol{a}/m]}$$
$$=\prod_{\mathcal{P}}\mathcal{P}^{\frac{N}{m}(\operatorname{ord}_{\mathcal{P}}a_1(m_1-1)+\cdots+\operatorname{ord}_{\mathcal{P}}a_n(m_n-1))-N+\frac{N}{m}(\operatorname{ord}_{\mathcal{P}}\boldsymbol{a},m)}. \blacksquare$$

The following result is a generalization of the orthogonality of roots of unity, for multi-index exponents.

LEMMA 9. *Let $\boldsymbol{r}\in\hat{\mathcal{R}}$. Then*

$$\sum_{\boldsymbol{l}\in\mathcal{R}}\zeta_m^{\boldsymbol{l}\cdot\boldsymbol{r}}=N\delta_{\boldsymbol{r}}=\begin{cases}N & \text{if } \boldsymbol{r}=0,\\ 0 & \text{if } \boldsymbol{r}\neq 0.\end{cases}$$

Proof. If $\boldsymbol{r}=0$ it is clear that $\sum_{l\in\mathcal{R}}\zeta_m^{\boldsymbol{l}\cdot\boldsymbol{r}}=|\mathcal{R}|=N$. If $\boldsymbol{r}\neq 0$ there exists $1\le j\le n$ such that $r_j\neq 0$. Then

$$\sum_{\boldsymbol{l}\in\mathcal{R}}\zeta_m^{\boldsymbol{l}\cdot\boldsymbol{r}}=\sum_{l_1,\dots,\hat{l}_j,\dots,l_n}\ \sum_{l_j\in\mathcal{R}_j}\zeta_m^{\sum_{i\neq j}l_ir_i}\zeta_m{}^{l_jr_j}$$
$$=\sum_{l_1,\dots,\hat{l}_j,\dots,l_n}\zeta_m^{\sum_{i\neq j}l_ir_i}\sum_{l_j\in\mathcal{R}_j}\zeta_m{}^{l_jr_j},$$

and it is clear that

$$\sum_{l_j\in\mathcal{R}_j}\zeta_m{}^{l_jr_j}=\sum_{k=0}^{m_j-1}\big(\zeta_m^{\frac{m}{m_j}}\big)^{kr_j}=\sum_{k=0}^{m_j-1}(\zeta_{m_j}^{r_j})^k=0$$

since $r_j\neq 0$. $\blacksquare$

PROPOSITION 10. *Let the notation be as above and let $\omega\in\mathcal{O}_L$,*

$$\omega=\sum_{\boldsymbol{k}\in\hat{\mathcal{R}}}c_{\boldsymbol{k}}\boldsymbol{\alpha}^{\boldsymbol{k}},\qquad c_{\boldsymbol{k}}\in K.$$

Then for $\boldsymbol{r}\in\hat{\mathcal{R}}$ we have $\omega_{\boldsymbol{r}}=Nc_{\boldsymbol{r}}\boldsymbol{\alpha}^{\boldsymbol{r}}$.

Moreover, let $\boldsymbol{a}=\boldsymbol{\alpha}^m\in\mathcal{O}_K^n$ and let $\mathcal{B}_{\boldsymbol{r}}$ be the ideals associated to $\boldsymbol{a}$. Then $Nc_{\boldsymbol{r}}\mathcal{B}_{\boldsymbol{r}}\subseteq\mathcal{O}_K$ for any $\boldsymbol{r}\in\hat{\mathcal{R}}$.

Proof. We have

$$\omega_{\boldsymbol{r}}=\sum_{\sigma\in G}\sigma(\omega)\overline{\boldsymbol{\chi}^{\boldsymbol{r}}(\sigma)}=\sum_{\boldsymbol{l}\in\mathcal{R}}\boldsymbol{\sigma}^{\boldsymbol{l}}(\omega)\overline{\boldsymbol{\chi}^{\boldsymbol{r}}(\boldsymbol{\sigma}^{\boldsymbol{l}})}=\sum_{\boldsymbol{l}\in\mathcal{R}}\sum_{\boldsymbol{k}\in\hat{\mathcal{R}}}c_{\boldsymbol{k}}\boldsymbol{\alpha}^{\boldsymbol{k}}\zeta_m^{\boldsymbol{l}\cdot(\boldsymbol{k}-\boldsymbol{r})}$$
$$=\sum_{\boldsymbol{k}\in\hat{\mathcal{R}}}c_{\boldsymbol{k}}\boldsymbol{\alpha}^{\boldsymbol{k}}\sum_{\boldsymbol{l}\in\mathcal{R}}\zeta_m^{\boldsymbol{l}\cdot(\boldsymbol{k}-\boldsymbol{r})}=Nc_{\boldsymbol{r}}\boldsymbol{\alpha}^{\boldsymbol{r}}\in\mathcal{O}_L.$$

Now, $Nc_{\boldsymbol{r}}\boldsymbol{\alpha}^{\boldsymbol{r}} \in \mathcal{O}_L$ implies that $(Nc_{\boldsymbol{r}}\boldsymbol{\alpha}^{\boldsymbol{r}})^m \in K \cap \mathcal{O}_L = \mathcal{O}_K$, hence

$$(Nc_{\boldsymbol{r}}\boldsymbol{\alpha}^{\boldsymbol{r}})^m\mathcal{O}_K = (Nc_{\boldsymbol{r}})^m\boldsymbol{a}^{\boldsymbol{r}}\mathcal{O}_K = (Nc_{\boldsymbol{r}})^m \prod_{\mathcal{P}} \mathcal{P}^{\boldsymbol{r}\cdot \mathrm{ord}_{\mathcal{P}}\,\boldsymbol{a}}\mathcal{O}_K \subseteq \mathcal{O}_K.$$

Moreover, as $(Nc_{\boldsymbol{r}})^m$ is an mth power, we also have

$$(Nc_{\boldsymbol{r}})^m \prod_{\mathcal{P}} \mathcal{P}^{[\boldsymbol{r}\cdot \mathrm{ord}_{\mathcal{P}}\,\boldsymbol{a}/m]\,m} \subseteq \mathcal{O}_K,$$

that is, $(Nc_{\boldsymbol{r}}\mathcal{B}_{\boldsymbol{r}})^m \subseteq \mathcal{O}_K$, thus $Nc_{\boldsymbol{r}}\mathcal{B}_{\boldsymbol{r}} \subseteq \mathcal{O}_K$. ∎

THEOREM 11. *Let L/K be a Kummer extension of exponent m and assume that L/K is tamely ramified. Then L/K has a NIB if and only if there exists a set of integral Kummer generators $\alpha_1, \dots, \alpha_n$ of L over K such that, putting $a_i = \alpha_i^m$, $\boldsymbol{a} = (a_1, \dots, a_n)$, $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$, $N = [L : K]$, the following conditions hold:*

(i) *the ideals $\mathcal{B}_{\boldsymbol{r}}$ associated to $\boldsymbol{a}$ are principal for any $\boldsymbol{r}$;*

(ii) *the congruence*

$$\sum_{\boldsymbol{r}\in\hat{\mathcal{R}}} \frac{\boldsymbol{\alpha}^{\boldsymbol{r}}}{x_{\boldsymbol{r}}} \equiv 0 \pmod{N}$$

holds for some $x_{\boldsymbol{r}} \in \mathcal{O}_K$, with $\mathcal{B}_{\boldsymbol{r}} = x_{\boldsymbol{r}}\mathcal{O}_K$.

Further, when this is the case, the integer

$$\omega = \frac{1}{N}\sum_{\boldsymbol{r}\in\hat{\mathcal{R}}} \frac{\boldsymbol{\alpha}^{\boldsymbol{r}}}{x_{\boldsymbol{r}}}$$

generates $\mathcal{O}_L$ over $\mathcal{O}_K[G]$.

Proof. Let $\alpha_1, \dots, \alpha_n$ be a set of integral Kummer generators of L over K satisfying (i) and (ii). Let $a_i = \alpha_i^m$, and let $x_{\boldsymbol{r}}$ and ω be as in the statement. Then, by Proposition 10, $\omega_{\boldsymbol{r}} = \langle \omega, \boldsymbol{\chi}^{\boldsymbol{r}} \rangle = \boldsymbol{\alpha}^{\boldsymbol{r}}/x_{\boldsymbol{r}}$.

It follows from Lemma 5 that

$$\mathrm{disc}_{L/K}(\mathcal{O}_K[G]\omega) = \prod_{\boldsymbol{r}\in\hat{\mathcal{R}}} \omega_{\boldsymbol{r}}^2\mathcal{O}_K = \frac{\prod_i \alpha_i^{N(m_i-1)}}{(\prod_{\boldsymbol{r}} x_{\boldsymbol{r}})^2}\mathcal{O}_K$$

$$= \frac{\prod_i a_i^{\frac{N}{m}(m_i-1)}}{(\prod_{\boldsymbol{r}} x_{\boldsymbol{r}})^2}\mathcal{O}_K = \prod_{\mathcal{P}} \mathcal{P}^{\frac{N}{m}(\mathrm{ord}_{\mathcal{P}}\, a_1(m_1-1)+\cdots+\mathrm{ord}_{\mathcal{P}}\, a_n(m_n-1))} \prod_{\boldsymbol{r}\in\hat{\mathcal{R}}} \mathcal{B}_{\boldsymbol{r}}^{-2},$$

and, by Corollary 8,

$$\mathrm{disc}_{L/K}(\mathcal{O}_K[G]\omega) = \prod_{\mathcal{P}} \mathcal{P}^{N-\frac{N}{m}(\mathrm{ord}_{\mathcal{P}}\,\boldsymbol{a},m)}. \tag{1}$$

The last equation and Corollary 4 show that

$$\mathrm{disc}(L/K) = \mathrm{disc}_{L/K}(\mathcal{O}_K[G]\omega),$$

and, since ω is an integer, this ensures that $\mathcal{O}_L = \mathcal{O}_K[G]\omega$.

Assume now that $\mathcal{O}_L = \mathcal{O}_K[G]\omega$, for some $\omega \in \mathcal{O}_L$. Let $\alpha_1, \dots, \alpha_n$ be a set of integral Kummer generators of L over K and put $a_i = \alpha_i^m \in \mathcal{O}_K$. Denote by $\mathcal{B}_{\boldsymbol{r}}$ the ideals associated to $\boldsymbol{a} = (a_1, \dots, a_n)$.

The set $\{\boldsymbol{\alpha}^{\boldsymbol{r}}\}_{\boldsymbol{r}\in\hat{\mathcal{R}}}$ is a K-basis of L, hence we can write $\omega = \sum_{\boldsymbol{r}\in\hat{\mathcal{R}}} c_{\boldsymbol{r}}\boldsymbol{\alpha}^{\boldsymbol{r}}$ with $c_{\boldsymbol{r}} \in K$, and, from Lemma 5 and Proposition 10, we get

$$\operatorname{disc}_{L/K}(\mathcal{O}_K[G]\omega) = \prod_{\boldsymbol{r}\in\hat{\mathcal{R}}} \omega_{\boldsymbol{r}}^2 \mathcal{O}_K = \prod_i a_i^{\frac{N}{m}(m_i-1)} \Big(\prod_{\boldsymbol{r}\in\hat{\mathcal{R}}} N c_{\boldsymbol{r}} \Big)^2 \mathcal{O}_K. \tag{2}$$

Since $\mathcal{O}_L = \mathcal{O}_K[G]\omega$, by comparing the values of the two discriminants given in (2) and in Corollary 4 we get

$$\prod_{\mathcal{P}} \mathcal{P}^{\frac{N}{m}(\operatorname{ord}_{\mathcal{P}} a_1(m_1-1)+\cdots+\operatorname{ord}_{\mathcal{P}} a_n(m_n-1))} \Big(\prod_{\boldsymbol{r}\in\hat{\mathcal{R}}} N c_{\boldsymbol{r}} \Big)^2 = \prod_{\mathcal{P}} \mathcal{P}^{N-\frac{N}{m}(\operatorname{ord}_{\mathcal{P}} \boldsymbol{a},m)},$$

or, equivalently,

$$\Big(\prod_{\boldsymbol{r}\in\hat{\mathcal{R}}} N c_{\boldsymbol{r}} \Big)^2 \prod_{\mathcal{P}} \mathcal{P}^{\frac{N}{m}(\operatorname{ord}_{\mathcal{P}} a_1(m_1-1)+\cdots+\operatorname{ord}_{\mathcal{P}} a_n(m_n-1))-N+\frac{N}{m}(\operatorname{ord}_{\mathcal{P}} \boldsymbol{a},m)} = \mathcal{O}_K,$$

and, using Corollary 8,

$$\prod_{\boldsymbol{r}\in\hat{\mathcal{R}}} N c_{\boldsymbol{r}} \mathcal{B}_{\boldsymbol{r}} = \mathcal{O}_K.$$

Now, from Proposition 10 we deduce that all the ideals $N c_{\boldsymbol{r}} \mathcal{B}_{\boldsymbol{r}}$ are integral ideals, so we must have $N c_{\boldsymbol{r}} \mathcal{B}_{\boldsymbol{r}} = \mathcal{O}_K$ for all $\boldsymbol{r} \in \hat{\mathcal{R}}$, i.e. $\mathcal{B}_{\boldsymbol{r}} = (N c_{\boldsymbol{r}})^{-1} \mathcal{O}_K$.

Finally, choosing $x_{\boldsymbol{r}} = (N c_{\boldsymbol{r}})^{-1}$ we get

$$\sum_{\boldsymbol{r}\in\hat{\mathcal{R}}} \frac{\boldsymbol{\alpha}^{\boldsymbol{r}}}{x_{\boldsymbol{r}}} = \sum_{\boldsymbol{r}\in\hat{\mathcal{R}}} N c_{\boldsymbol{r}} \boldsymbol{\alpha}^{\boldsymbol{r}} = N\omega \equiv 0 \pmod{N}. \ \blacksquare$$

COROLLARY 12. *Let $L = K(\sqrt{\boldsymbol{a}})$ with $(a_i, m) = 1$ for all i, and assume that conditions* (i) *and* (ii) *of Theorem* 11 *hold for L/K. Then L/K is tame and has a NIB.*

Proof. Let

$$\omega = \frac{1}{N} \sum_{\boldsymbol{r}\in\hat{\mathcal{R}}} \frac{\boldsymbol{\alpha}^{\boldsymbol{r}}}{x_{\boldsymbol{r}}},$$

as in the theorem. We note that equation (1) does not depend on tame ramification; hence, also in this case we have

$$\operatorname{disc}_{L/K}(\mathcal{O}_K[G]\omega) = \prod_{\mathcal{P}} \mathcal{P}^{N-\frac{N}{m}(\operatorname{ord}_{\mathcal{P}} \boldsymbol{a},m)}.$$

Now, as $(a_i, m) = 1$ for all i, the last equation ensures that $\operatorname{disc}_{L/K}(\mathcal{O}_K[G]\omega)$ is coprime to m; since $\omega \in \mathcal{O}_L$ it is clear that

$$\operatorname{disc}(L/K) \mid \operatorname{disc}_{L/K}(\mathcal{O}_K[G]\omega),$$

thus L/K is tamely ramified. The existence of the NIB follows from Theorem 11. ∎

Let L/K be a number field extension, let $v_1, \dots, v_n$ be a K-basis of L and let $\mathcal{I}$ be the fractional ideal of $\mathcal{O}_K$ such that

$$\operatorname{disc}(L/K) = \mathcal{I}^2 \operatorname{disc}_{L/K}(v_1, \dots, v_n).$$

We recall that the *Steinitz class* of the extension L/K is the class of $\mathcal{I}$ in the ideal class group of K. The following proposition generalizes [5, Prop. 2.5] and [3, Prop. 1].

Proposition 13. *Let L/K be a tame Kummer extension of exponent m, let $\boldsymbol{a} \in \mathcal{O}_K^n$ be such that $L = K(\sqrt[m]{\boldsymbol{a}})$ and let $\mathcal{B}_{\boldsymbol{r}}$ be the ideals associated to $\boldsymbol{a}$. Then the Steinitz class of L/K is the ideal class of $(\prod_{\boldsymbol{r}\in\hat{\mathcal{R}}} \mathcal{B}_{\boldsymbol{r}})^{-1}$. In particular, $\mathcal{O}_L$ is free over $\mathcal{O}_K$ if and only if the ideal $\prod_{\boldsymbol{r}\in\hat{\mathcal{R}}} \mathcal{B}_{\boldsymbol{r}}$ is principal.*

Proof. Since the extension is tamely ramified, by Corollary 4 we have

$$\operatorname{disc}(L/K) = \prod_{\mathcal{P}} \mathcal{P}^{N - \frac{N}{m}(\operatorname{ord}_{\mathcal{P}} \boldsymbol{a}, m)}.$$

On the other hand, the discriminant $\operatorname{disc}_{L/K}\{(\sqrt[m]{\boldsymbol{a}^{\boldsymbol{r}}})_{\boldsymbol{r}\in\hat{\mathcal{R}}}\}$ is the square of the determinant of the matrix $\{\sigma^{\mathbf{l}}(\sqrt[m]{\boldsymbol{a}^{\boldsymbol{r}}})\}$ and this matrix is the tensor product (or Kronecker product) of the matrices $\{\sigma_i^{l_i}(\sqrt[m]{a_i^{r_i}})\}$ for $i = 1, \dots, n$. It follows (see for example [1, Prop. 2.14]) that

$$\operatorname{disc}_{L/K}(\sqrt[m]{\boldsymbol{a}^{\boldsymbol{r}}})_{\boldsymbol{r}\in\hat{\mathcal{R}}} = \prod_{i=1}^{n} \left[\operatorname{disc}_{K(\sqrt[m]{a_i})/K} \left(1, \sqrt[m]{a_i}, \sqrt[m]{a_i}^2, \dots, \sqrt[m]{a_i}^{m_i-1}\right)\right]^{N/m_i}.$$

We recall that $\tilde{a}_i := a_i^{m_i/m} \in K$ and $K(\sqrt[m]{a_i}) = K(\sqrt[m_i]{\tilde{a}_i})$, thus the standard discriminant calculation gives

$$\operatorname{disc}_{K(\sqrt[m]{a_i})/K} \left(1, \sqrt[m]{a_i}, \sqrt[m]{a_i}^2, \dots, \sqrt[m]{a_i}^{m_i-1}\right) = m_i^{m_i} a_i^{\frac{m_i}{m}(m_i-1)}.$$

Hence we have

$$\begin{aligned}\operatorname{disc}_{L/K}(\sqrt[m]{\boldsymbol{a}^{\boldsymbol{r}}})_{\boldsymbol{r}\in\hat{\mathcal{R}}} &= \prod_{i=1}^{n} (m_i^{m_i} a_i^{\frac{m_i}{m}(m_i-1)})^{N/m_i} \mathcal{O}_K = N^N \prod_{i=1}^{n} a_i^{\frac{N}{m}(m_i-1)} \mathcal{O}_K \\ &= N^N \prod_{\mathcal{P}} \mathcal{P}^{\sum_i \frac{N}{m} \operatorname{ord}_{\mathcal{P}}(a_i)(m_i-1)},\end{aligned}$$

thus

$$\mathcal{I}^{-2} = N^N \prod_{\mathcal{P}} \mathcal{P}^{\sum_i \frac{N}{m} \operatorname{ord}_{\mathcal{P}}(a_i)(m_i-1) - N + \frac{N}{m}(\operatorname{ord}_{\mathcal{P}} \boldsymbol{a}, m)},$$

and, by Corollary 8,

$$\mathcal{I}^{-2} = N^N \prod_{\boldsymbol{r}\in\hat{\mathcal{R}}} \mathcal{B}_{\boldsymbol{r}}^2.$$

If N is even we have

$$\mathcal{I}^{-1} = N^{N/2} \prod_{\boldsymbol{r}\in\hat{\mathcal{R}}} \mathcal{B}_{\boldsymbol{r}};$$

if N is odd we have

$$N\mathcal{O}_K = p_1^{a_1}\cdots p_r^{a_r}\mathcal{O}_K = (1-\zeta_{p_1})^{(p_1-1)a_1}\cdots(1-\zeta_{p_r})^{(p_r-1)a_r}\mathcal{O}_K$$

with p_i odd primes, hence

$$\mathcal{I}^{-1} = (1-\zeta_{p_1})^{(p_1-1)a_1/2}\cdots(1-\zeta_{p_r})^{(p_r-1)a_r/2} \prod_{\boldsymbol{r}\in\hat{\mathcal{R}}} \mathcal{B}_{\boldsymbol{r}}.$$

In both cases it is clear that the class of $\mathcal{I}$ coincides with the class of $\left(\prod_{\boldsymbol{r}\in\hat{\mathcal{R}}} \mathcal{B}_{\boldsymbol{r}}\right)^{-1}$. ∎

3. The case $\mathbb{Q}(\zeta_m, \sqrt[m]{\boldsymbol{a}})$. In this section we study the particular case of extensions $\mathbb{Q}(\zeta_m, \sqrt[m]{\boldsymbol{a}})$ with $\boldsymbol{a} = \{a_1, \dots, a_n\} \subset \mathbb{Q}$. In the first subsection, we give necessary and sufficient explicit conditions for these kind of extensions to be tamely ramified, the final result being contained in Proposition 24 and in Corollary 25. In the second subsection, we prove that in the case of tame ramification, these extensions always have an integral basis; this is equivalent to the Steinitz class of the extension being trivial (see the end of Section 2). In the third subsection, we study the problem of the existence of a normal integral basis in the case when the exponent m of the extension is square-free and $(a_i, m) = 1$ for all i; we show that, for non-cyclic extensions, tame ramification is not a sufficient condition. In the last subsection, we present further examples.

3.1. Tameness conditions. In the following we study the ramification in extensions $\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}(\zeta_m)$, with $a \in \mathbb{Q}$. The goal is Proposition 24, in which we give an explicit criterion for tame ramification in such extensions.

Lemma 14 ([12, Ch. 6, Thm. 9.1]). *Let F be a field and let $n \geq 2$. Let $a \in F^*$ and assume that for all prime numbers p such that $p \mid n$ we have $a \notin (F^*)^p$, and if $4 \mid n$ then $a \notin -4(F^*)^4$. Then $x^n - a$ is irreducible in $F[x]$.* ∎

Corollary 15. *Let p be an odd prime and let F be a p-adic field such that $\zeta_p \notin F$. Let $b \in F^* \setminus (F^*)^p$ and let $\beta \in \bar{\mathbb{Q}}_p$ such that $\beta^p = b$. Then $F(\beta)/F$ has degree p and it is not normal.*

Proof. This immediately follows from the lemma and the assumption $\zeta_p \notin F$. ∎

Lemma 16. *Let p be an odd prime and let F be a p-adic field such that $\zeta_p \notin F$. Let $k, n \in \mathbb{N}$ with $k \leq n$, and let $b \in F$ and $\beta \in \bar{F}$ be such that*

$\beta^{p^k} = b$. *Then*

$$[F(\zeta_{p^n}, \beta) : F(\zeta_{p^n})] = [F(\beta) : F].$$

In particular, if $b \in F^* \setminus (F^*)^p$, *then* $[F(\zeta_{p^n}, \sqrt[p^k]{b}) : F(\zeta_{p^n})] = p^k$.

Proof. Clearly if $b \in (F^*)^{p^k}$ both extensions are trivial. Assume now that $b \notin (F^*)^{p^k}$. Let $r \in \{0, \dots, k-1\}$ be such that $b \in (F^*)^{p^r} \setminus (F^*)^{p^{r+1}}$, let $c \in F \setminus (F^*)^p$ be such that $c^{p^r} = b$ and let $s = k - r$. With this notation, we have $\beta^{p^s} = c$, hence $[F(\beta) : F] = p^s$.

On the other hand, by Kummer theory, $F(\zeta_{p^n}, \beta) = F(\zeta_{p^n}, \sqrt[p^s]{c})$ has degree p^s unless $\gamma = \sqrt[p]{c} \in F(\zeta_{p^n})$; however, the last condition cannot hold since it would imply that $F \subset F(\gamma) \subset F(\zeta_{p^n})$, but $F(\zeta_{p^n})/F$ is cyclic, whereas, by Corollary 15, $F(\gamma)/F$ is not normal. ∎

Lemma 17. *Let* p *be an odd prime and let* F *be a* p*-adic field with ramification index over* $\mathbb{Q}_p$ *coprime to* p. *Let* $k, n \in \mathbb{N}$ *with* $k \leq n$ *and let* $b \in F^*$. *Then the extension* $F(\zeta_{p^n}, \sqrt[p^k]{b})/F(\zeta_{p^n})$ *is totally ramified and not trivial if* $b \notin (F^*)^{p^k}$, *and it is trivial if* $b \in (F^*)^{p^k}$.

Proof. Clearly if $b \in (F^*)^{p^k}$ the extension is trivial. Assume now that $b \notin (F^*)^{p^k}$. Let $r \in \{0, \dots, k-1\}$ be such that $b \in (F^*)^{p^r} \setminus (F^*)^{p^{r+1}}$, let $c \in F \setminus (F^*)^p$ be such that $c^{p^r} = b$ and let $s = k - r$. With this notation, $F(\zeta_{p^n}, \sqrt[p^k]{b}) = F(\zeta_{p^n}, \sqrt[p^s]{c})$ is a cyclic extension of $F(\zeta_{p^n})$ and, by Lemma 16, it has degree $p^s > 1$.

We claim that this extension is totally ramified. If not, its degree p subextension $F(\zeta_{p^n}, \sqrt[p]{c})/F(\zeta_{p^n})$ would be unramified. Denote by U the degree p unramified extension of F; then $U \subseteq F(\zeta_{p^n}, \sqrt[p]{c})$. Moreover, our hypothesis on the ramification index of F guarantees that $F(\zeta_{p^n}) \cap U = F$ and $F(\zeta_{p^n}, \sqrt[p]{c}) = F(\zeta_{p^n})U$, and this implies that $F(\zeta_{p^n}, \sqrt[p]{c})/F$ is abelian since it is the compositum of two linearly disjoint abelian extensions of F. This gives a contradiction since, by Corollary 15, the subextension $F(\sqrt[p]{c})/F$ is not normal. ∎

Corollary 18. *Let* $m, k \in \mathbb{N}$, *let* p *be an odd prime number and assume* $p^k \mid m$. *Let* F *be a* p*-adic field with ramification index over* $\mathbb{Q}_p$ *coprime to* p, *and let* $b \in F^*$. *Then the extension* $F(\zeta_m, \sqrt[p^k]{b})/F(\zeta_m)$ *is totally ramified and not trivial if* $b \notin (F^*)^{p^k}$, *and it is trivial if* $b \in (F^*)^{p^k}$.

Proof. Let $m = p^n m'$ with $(m', p) = 1$, then $n \geq k$. The corollary follows from observing that $F(\zeta_m, \sqrt[p^k]{b})/F(\zeta_m)$ is the translate of $F(\zeta_{p^n}, \sqrt[p^k]{b})/F(\zeta_{p^n})$ by the unramified extension $F(\zeta_{m'})$ and from Lemma 17. ∎

For simplicity of notation the following proposition is stated in the case when the base field is $\mathbb{Q}$. However, it is easy to extend it to a number field with ramification index over $\mathbb{Q}$ coprime to m.

PROPOSITION 19. *Let $m \in \mathbb{N}$ be an odd number, let $m = p_1^{n_1} \cdots p_r^{n_r}$ be its factorization into prime numbers and let $a \in \mathbb{Q}^*$. Then*

$$\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}(\zeta_m) \text{ is tamely ramified } \Leftrightarrow \ a \in (\mathbb{Q}_{p_i}^*)^{p_i^{n_i}} \text{ for all } i = 1, \dots, r.$$

Proof. The extension $\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}(\zeta_m)$ is a Kummer extension and its degree is a divisor of m. It follows that it is tamely ramified if and only if the primes over the p_i are tamely ramified. Since ramification is a local property, this is equivalent to the extensions $\mathbb{Q}_{p_i}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}_{p_i}(\zeta_m)$ being tame for $i = 1, \dots, r$.

Assume that $a \in (\mathbb{Q}_{p_i}^*)^{p_i^{n_i}}$ for all $i = 1, \dots, r$; clearly we have $\mathbb{Q}_{p_i}(\zeta_m) = \mathbb{Q}_{p_i}(\zeta_m, \sqrt[p_i^{n_i}]{a})$ for all i. It follows that $\mathbb{Q}_{p_i}(\zeta_m, \sqrt[m]{a}) = \mathbb{Q}_{p_i}(\zeta_m, \sqrt[m_i]{b_i})$ (where $b_i \in \mathbb{Q}_{p_i}$ is such that $a = b^{p_i^{n_i}}$ and $m_i = m/p_i^{n_i}$), and this extension is tamely ramified over $\mathbb{Q}_{p_i}(\zeta_m)$ since its degree is coprime to p_i.

Conversely, assume that the extensions $\mathbb{Q}_{p_i}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}_{p_i}(\zeta_m)$ are tame for $i = 1, \dots, r$; then the subextensions $\mathbb{Q}_{p_i}(\zeta_m, \sqrt[p_i^{n_i}]{a})/\mathbb{Q}_{p_i}(\zeta_m)$ are tamely ramified: since the degree of each of these extensions is a power of p, these extensions are tame if and only if they are unramified and, by Corollary 18, if and only if $a \in (\mathbb{Q}_{p_i}^*)^{p_i^{n_i}}$ for all $i = 1, \dots, r$. ∎

In the case $p = 2$ the situation is a bit different, and this is due to the fact that $\zeta_2 \in \mathbb{Q}_2$.

LEMMA 20. *Let $b \in \mathbb{Q}_2^* \setminus \pm(\mathbb{Q}_2^*)^2$ and let $\beta \in \bar{\mathbb{Q}}_2$ be such that $\beta^4 = b$. Then $\mathbb{Q}_2(\beta)/\mathbb{Q}_2$ is not normal.*

Proof. By Lemma 14, our choice of b guarantees that the polynomial $x^4 - b$ is irreducible, so its splitting field is $\mathbb{Q}_2(\beta, i)$. It follows that, if $\mathbb{Q}_2(\beta)/\mathbb{Q}_p$ is normal, then $i \in \mathbb{Q}_2(\beta)$ and, by Kummer theory, b is a square in $\mathbb{Q}_2(i)$. This cannot occur since $b \notin \pm(\mathbb{Q}_2^*)^2$. ∎

LEMMA 21. *Let $b \in \mathbb{Q}_2^*$ and let $n \geq 3$. The extension $\mathbb{Q}_2(\zeta_{2^n}, \sqrt{b})/\mathbb{Q}_2(\zeta_{2^n})$ is unramified or trivial according to whether $b \in \pm 5(\mathbb{Q}_2^*)^2 \cup \pm 10(\mathbb{Q}_2^*)^2$ or $b \in \pm(\mathbb{Q}_2^*)^2 \cup \pm 2(\mathbb{Q}_2^*)^2$.*

For $n = 2$, the extension $\mathbb{Q}_2(\zeta_4, \sqrt{b})/\mathbb{Q}_2(\zeta_4)$ is trivial when $b \in \pm(\mathbb{Q}_2^*)^2$, unramified when $b \in \pm 5(\mathbb{Q}_2^*)^2$, and totally ramified when $b \in \pm 2(\mathbb{Q}_2^*)^2 \cup \pm 10(\mathbb{Q}_2^*)^2$.

Proof. This follows easily by combining the following three facts: -1 and 2 are squares in $\mathbb{Q}_2(\zeta_8)$, the maximal abelian extension of exponent 2 of $\mathbb{Q}_2$ is $\mathbb{Q}_2(i, \sqrt{2}, \sqrt{5})$, and the unramified extension of degree 2 of $\mathbb{Q}_2$ is $\mathbb{Q}_2(\sqrt{5})$. ∎

LEMMA 22. *Let $b \in \mathbb{Q}_2^*$, let $k, n \in \mathbb{N}$ with $n \geq k \geq 1$ and denote by f the inertia degree of the extension $\mathbb{Q}_2(\zeta_{2^n}, \sqrt[2^k]{b})/\mathbb{Q}_2(\zeta_{2^n})$. Then $f \leq 2$.*

Proof. Let $l \le k$ be such that $\mathbb{Q}_2(\zeta_{2^n}, \sqrt[2^l]{b})$ is the maximal unramified subextension of $\mathbb{Q}_2(\zeta_{2^n}, \sqrt[2^k]{b})/\mathbb{Q}_2(\zeta_{2^n})$; we note that we can assume that $n > l$: in fact, otherwise we can translate the extension $\mathbb{Q}_2(\zeta_{2^n}, \sqrt[2^l]{b})/\mathbb{Q}_2(\zeta_{2^n})$ by $\mathbb{Q}_2(\zeta_{2^{n+1}})$ and this does not change the inertia degree. In this case we have $\mathbb{Q}_2(\zeta_{2^n}, \sqrt[2^l]{b}) = \mathbb{Q}_2(\zeta_{2^n}, \sqrt[2^l]{-b})$, so, by changing, if necessary, b to $-b$ and to its square root repeatedly, we can assume $b \notin \pm\mathbb{Q}_2^{*2}$.

Denote by U the unramified extension of $\mathbb{Q}_2$ of degree f. If $f \ge 4$ then necessarily $2^l \ge 4$, hence, letting $\beta \in \bar{\mathbb{Q}}_2$ be such that $\beta^4 = b$, we would have $\beta \in \mathbb{Q}_2(\zeta_{2^n})U$ and its Galois group would be abelian, whereas $\mathbb{Q}_2(\beta)$ is not normal over $\mathbb{Q}_2$ by Lemma 20 since $b \notin \pm\mathbb{Q}_2^{*2}$. ∎

LEMMA 23. *Let $b \in \mathbb{Q}_2^*$ and let $n \in \mathbb{N}$ with $n \ge 3$. Then the extension $\mathbb{Q}_2(\zeta_{2^n}, \sqrt[2^n]{b})/\mathbb{Q}_2(\zeta_{2^n})$ is tame if and only if $b \in (\mathbb{Q}_2^*)^{2^{n-1}}$.*

The extension $\mathbb{Q}_2(\zeta_4, \sqrt[4]{b})/\mathbb{Q}_2(\zeta_4)$ is tame if and only if either $b \in (\mathbb{Q}_2^*)^4 \cup -4(\mathbb{Q}_2^*)^4$, in which case the extension is trivial, or $b \in 25(\mathbb{Q}_2^*)^4 \cup -100(\mathbb{Q}_2^*)^4$, in which case $f = 2$.

Proof. Let us first consider the case $n \ge 3$.

If $b \in (\mathbb{Q}_2^*)^{2^{n-1}}$, then $b = c^{2^{n-1}}$ in $\mathbb{Q}_2$ and by Lemma 21 the extension $\mathbb{Q}_2(\zeta_{2^n}, \sqrt[2]{c})/\mathbb{Q}_2(\zeta_{2^n})$ is always unramified.

Assume now that the extension is tame; in this case the extension is necessarily unramified and by Lemma 22 it has degree at most 2. It follows that $\mathbb{Q}_2(\zeta_{2^n}, \sqrt[2^n]{b})$ is abelian over $\mathbb{Q}_2$ since it is a subextension of $\mathbb{Q}_2(\zeta_{2^n}, \sqrt{5})$, hence $\mathbb{Q}_2(\sqrt[2^n]{b})$ and all its subextensions are normal and abelian over $\mathbb{Q}_2$; by Lemma 20 this implies that $b \in \pm\mathbb{Q}_2^{*2}$.

Case $b \in \mathbb{Q}_2^{*2}$: let $r \ge 1$ be such that $b \in \mathbb{Q}_2^{*2^r} \setminus \mathbb{Q}_2^{*2^{r+1}}$; then $b = c^{2^r}$ with $c \notin \mathbb{Q}_2^{*2}$. We want to show that $r \ge n-1$, or, equivalently, that $s = n - r \le 1$. If $s \ge 2$ then $\sqrt[4]{c} \in \mathbb{Q}_2(\zeta_{2^n}, \sqrt{5})$, so $\mathbb{Q}_2(\sqrt[4]{c})/\mathbb{Q}_2$ is normal; by Lemma 20 and our choice of c we have $c \in -\mathbb{Q}_2^{*2}$, that is, $c = -d^2$ with $d \in \mathbb{Q}_2^*$. Now $b = (-d^2)^{2^r} = d^{2^{r+1}}$, since $r \ge 1$, and this is not possible, so $b \in (\mathbb{Q}_2^*)^{2^{n-1}}$.

Case $b \in -\mathbb{Q}_2^2$: we want to show that this case is not possible. Let $b' = -b$; then $\mathbb{Q}_2(\zeta_{2^{n+1}}, \sqrt[2^n]{b'}) = \mathbb{Q}_2(\zeta_{2^{n+1}}, \sqrt[2^n]{b})$, hence this extension is abelian over $\mathbb{Q}_2$. It follows that $\mathbb{Q}_2(\sqrt[2^n]{-b})/\mathbb{Q}_2$ is normal, and, taking into account that $b' \in \mathbb{Q}_2^{*2}$, arguing as before we get $b' \in (\mathbb{Q}_2^*)^{2^{n-1}}$, so $b = -c^{2^{n-1}}$ with $c \in \mathbb{Q}_2^*$.

We want to show that $\mathbb{Q}_2(\zeta_{2^n}, \sqrt[2^n]{-c^{2^{n-1}}}) = \mathbb{Q}_2(\zeta_{2^n}, \sqrt{(\zeta_{2^n} c)})$ cannot be contained in $\mathbb{Q}_2(\zeta_{2^n}, \sqrt{5})$. In fact, otherwise we would have $\zeta_{2^n} c 5^\epsilon \in \mathbb{Q}_2(\zeta_{2^n})^{*2}$ (with $\epsilon = 0, 1$ depending on the extension being trivial or of degree 2 over $\mathbb{Q}_2(\zeta_{2^n})$). Now $\mathbb{Q}_2^* = \langle 2 \rangle \times \langle -1 \rangle \times \langle 5 \rangle$ so $\zeta_{2^n} c 5^\epsilon = \zeta_{2^n} 2^g (-1)^h 5^{j+\epsilon}$ and since $n \ge 3$ the elements -1 and 2 are squares in $\mathbb{Q}_2(\zeta_{2^n})$, so $\zeta_{2^n} c 5^\epsilon$ can be a square in $\mathbb{Q}_2(\zeta_{2^n})$ only if at least one of ζ_{2^n}, $\zeta_{2^n} 5$ is a square in $\mathbb{Q}_2(\zeta_{2^n})$, which is not the case. In fact, this is clear for ζ_{2^n}, whereas for $\zeta_{2^n} 5$ it can

be seen by noting that $\zeta_{2^n}5 \in \mathcal{U}_1 \setminus \mathcal{U}_2$ so it cannot belong to $\mathcal{U}_1^2$ (here $\mathcal{U}_i = \mathcal{U}_i(\mathbb{Q}_2(\zeta_{2^n})) = \{x \in \mathbb{Q}_2(\zeta_{2^n})^* \mid x \equiv 1 \pmod{(\zeta_{2^n}-1)^i}\}$ and we are using that for a local field K we have $K^* \cong \mathbb{Z} \times \mathbb{F}_{q_K}^* \times \mathcal{U}_1$, see for example [14, Cor. 1 p. 216]).

The case $n = 2$ can be easily proved by direct computation or consulting a database (for example [9]). ∎

Finally it is clear that an analogue of Corollary 18 holds also for $p = 2$, hence the previous result allows us to generalize Proposition 19 to all natural numbers.

PROPOSITION 24. *Let $m \in \mathbb{N}$ and let $m = 2^n p_1^{n_1} \cdots p_r^{n_r}$ be its factorization into primes, where $n \geq 0$ and $n_i > 0$ for all i. For $a \in \mathbb{Q}^*$, $\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}(\zeta_m)$ is tamely ramified if and only if $a \in (\mathbb{Q}_{p_i}^*)^{p_i^{n_i}}$ for all $i = 1, \ldots, r$ and, if m is even, one of the following conditions hold:*

- *$n = 1$ and $a \in (\mathbb{Q}_2^*)^2 \cup 5(\mathbb{Q}_2^*)^2$;*
- *$n = 2$ and $a \in (\mathbb{Q}_2^*)^4 \cup -4(\mathbb{Q}_2^*)^4 \cup 25(\mathbb{Q}_2^*)^4 \cup -100(\mathbb{Q}_2^*)^4$;*
- *$n \geq 3$ and $a \in (\mathbb{Q}_2^*)^{2^{n-1}}$.*

COROLLARY 25. *Let $m \in \mathbb{N}$ and let $m = p_1^{n_1} \cdots p_r^{n_r}$ be its factorization into prime numbers. For any $a \in \mathbb{Z}$ such that $(a, m) = 1$,*

$$\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}(\zeta_m) \text{ is tamely ramified} \Leftrightarrow a^{p_i-1} \equiv 1 \pmod{p_i^{n_i+1}} \ \forall i = 1, \ldots, r.$$

Proof. We have to show that the conditions of Proposition 24 become those of the statement when a is an integer coprime to m.

Let us first consider the case of an odd prime p such that $(a, p) = 1$: we have to prove that $a \in (\mathbb{Q}_p^*)^{p^n} \Leftrightarrow a^{p-1} \equiv 1 \pmod{p^{n+1}}$.

We recall that $\mathbb{Q}_p^* \cong \langle p \rangle \times \langle \omega \rangle \times U_1$ where ω is a primitive $(p-1)$th root of unity and $U_1 = \{x \in \mathbb{Z}_p \mid x \equiv 1 \pmod{p}\}$. It follows that $(\mathbb{Q}_p^*)^{p^n} \cong \langle p^{p^n} \rangle \times \langle \omega \rangle \times U_1^{p^n}$. Since $(a, p) = 1$, in $\mathbb{Q}_p^*$ we have $a = \omega^i u$ with $u \in U_1$. It follows that $a \in (\mathbb{Q}_p^*)^{p^n}$ if and only if $u \in U_1^{p^n}$, namely if and only if $u \equiv 1 \pmod{p^{n+1}}$ (this can be easily seen by direct computation or deduced from general results like [14, Corollary p. 217]). Since $\omega^{p-1} = 1$ the result follows.

Let us now consider the case $p = 2$; let n be the exponent of 2 in the factorization of m. We recall that $\mathbb{Q}_2^* \cong \langle 2 \rangle \times U_1 = \langle 2 \rangle \times \langle -1 \rangle \times U_2$.

If $n = 1$, from Proposition 24 we see that 2 is tamely ramified if and only if $a \in (\mathbb{Q}_2^*)^2 \cup 5(\mathbb{Q}_2^*)^2$. Now $a \in (\mathbb{Q}_2^*)^2$ if and only if $a \equiv 1 \pmod 8$ and $a \in 5(\mathbb{Q}_2^*)^2$ if and only if $a \equiv 5 \pmod 8$, thus 2 is tamely ramified if and only if $a \equiv 1 \pmod{4 = 2^{n+1}}$.

If $n = 2$, from Proposition 24 we infer that 2 is tamely ramified if and only if $a \in (\mathbb{Q}_2^*)^4 \cup -4(\mathbb{Q}_2^*)^4 \cup 25(\mathbb{Q}_2^*)^4 \cup -100(\mathbb{Q}_2^*)^4$; since $(a, 2) = 1$ we have

to consider the case $a \in (\mathbb{Q}_2^*)^4 \cup 25(\mathbb{Q}_2^*)^4$. Now $a \in (\mathbb{Q}_2^*)^4$ if and only if $a \equiv 1 \pmod{16}$, and $a \in 25(\mathbb{Q}_2^*)^4$ if and only if $a \equiv 25 \equiv 9 \pmod{16}$, thus 2 is tamely ramified if and only if $a \equiv 1 \pmod{8 = 2^{n+1}}$.

If $n \geq 3$, from Proposition 24 we conclude that 2 is tamely ramified if and only if $a \in (\mathbb{Q}_2^*)^{2^{n-1}}$, that is, if and only if $a \equiv 1 \pmod{2^{n+1}}$. ∎

3.2. The Steinitz class. In this part we prove that tame extensions of the kind $\mathbb{Q}(\zeta_m, \sqrt[m]{\boldsymbol{a}})/\mathbb{Q}(\zeta_m)$ always have an integral basis.

We begin by recalling the definition of ambiguous ideals: Let K/F be a Galois extension of number fields. Then a fractional ideal $\mathcal{I}$ of K is called an *ambiguous ideal* of K/F if it is invariant under the action of $\mathrm{Gal}(K/F)$. Since the orbit of a prime $\mathcal{P}$ of $\mathcal{O}_K$ under the action of $\mathrm{Gal}(K/F)$ consists of all the primes of $\mathcal{O}_K$ lying over $P = \mathcal{P} \cap \mathcal{O}_F$, using the unique factorization property it is easy to see that $\mathcal{I}$ is an ambiguous ideal of K/F if and only if

$$\mathcal{I} = \prod_{\substack{P \subseteq \mathcal{O}_F \\ P \text{ prime}}} \sqrt{P\mathcal{O}_K}^{\,n_P}, \tag{3}$$

where $\sqrt{P\mathcal{O}_K}$ denotes the radical of the ideal $P\mathcal{O}_K$, that is, the product of all the primes of $\mathcal{O}_K$ over P, and the n_P's are integers, all but a finite number trivial.

Lemma 26. *Let $m \geq 2$ be a positive integer and $\boldsymbol{a} = (a_1, \dots, a_n) \in \mathbb{Z}^n$. Then, for all $\boldsymbol{r} \in \hat{\mathcal{R}}$, the ideal $\mathcal{B}_{\boldsymbol{r}}$ associated to $\boldsymbol{a}$ in the extension $\mathbb{Q}(\zeta_m, \sqrt[m]{\boldsymbol{a}})/\mathbb{Q}(\zeta_m)$ is an ambiguous ideal of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$.*

Proof. Let $K := \mathbb{Q}(\zeta_m)$. For $\boldsymbol{r} \in \hat{\mathcal{R}}$ we have

$$\mathcal{B}_{\boldsymbol{r}} = \prod_{\mathcal{P} \subset \mathcal{O}_K} \mathcal{P}^{[\frac{\boldsymbol{r} \cdot \mathrm{ord}_{\mathcal{P}} \boldsymbol{a}}{m}]} = \prod_{\substack{p \in \mathbb{Z} \\ p \text{ prime}}} \prod_{\mathcal{P} \mid p} \mathcal{P}^{[\frac{\boldsymbol{r} \cdot \mathrm{ord}_{\mathcal{P}} \boldsymbol{a}}{m}]}.$$

By (3) we have to prove that the number $\left[\frac{\boldsymbol{r} \cdot \mathrm{ord}_{\mathcal{P}} \boldsymbol{a}}{m}\right] = \left[\sum_{i=1}^n \frac{r_i \,\mathrm{ord}_{\mathcal{P}} a_i}{m}\right]$ does not depend on $\mathcal{P}$, but only on $p = \mathcal{P} \cap \mathbb{Z}$. Since $a_i \in \mathbb{Z}$ for all i, it is clear that $\mathrm{ord}_{\mathcal{P}} a_i = e_{\mathcal{P}} \,\mathrm{ord}_p a_i$ but, $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ being a Galois extension, $e_{\mathcal{P}}$ depends only on the prime p lying under $\mathcal{P}$. Putting $e_{\mathcal{P}} = e_p$, we get

$$\mathcal{B}_{\boldsymbol{r}} = \prod_{\substack{p \in \mathbb{Z} \\ p \text{ prime}}} \prod_{\mathcal{P} \mid p} \mathcal{P}^{\left[\frac{e_p (\boldsymbol{r} \cdot \mathrm{ord}_p \boldsymbol{a})}{m}\right]} = \prod_{\substack{p \in \mathbb{Z} \\ p \text{ prime}}} \sqrt{p\mathcal{O}_K}^{\left[\frac{e_p (\boldsymbol{r} \cdot \mathrm{ord}_p \boldsymbol{a})}{m}\right]}, \tag{4}$$

as required. ∎

Lemma 27. *All ambiguous ideals of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ are principal.*

Proof. Let $K := \mathbb{Q}(\zeta_m)$; by (3) it is sufficient to show that $\sqrt{p\mathcal{O}_K}$ is principal for any rational prime p. If $p \nmid m$, then p is unramified in $\mathcal{O}_K$, thus

$\sqrt{p\mathcal{O}_K} = p\mathcal{O}_K$ is principal. If $p \mid m$, let $m = p^{n_p}\nu_p$ with $(p, \nu_p) = 1$. Then

$$\sqrt{p\mathcal{O}_K} = (\zeta_{p^{n_p}} - 1)\mathcal{O}_K,$$

hence also in this case $\sqrt{p\mathcal{O}_K}$ is principal, and the lemma follows. ∎

COROLLARY 28. *Let the notation be as in Lemma* 26. *For all* $\boldsymbol{r} \in \hat{\mathcal{R}}$ *the ideal* $\mathcal{B}_{\boldsymbol{r}}$ *associated to* $\boldsymbol{a}$ *is principal; moreover, if* $(a_i, m) = 1$ *for all* $i = 1, \dots, n$, *all of the* $\mathcal{B}_{\boldsymbol{r}}$*'s are generated by rational integers coprime to* m.

Proof. The first assertion immediately follows from Lemmas 26 and 27. Moreover, the primes which really appear in the product in (4) are those dividing $\tilde{a} := a_1 \dots a_n$. It follows that, if $(\tilde{a}, m) = 1$, then the primes which appear in the product do not divide m, hence in this case $\sqrt{p\mathcal{O}_K} = p\,\mathcal{O}_K$ and

$$\mathcal{B}_{\boldsymbol{r}} = \prod_{\substack{p \text{ prime} \\ p \mid \tilde{a}}} p^{[\frac{r \cdot \operatorname{ord}_p a}{m}]}\mathcal{O}_K$$

is generated by an integer coprime to m. ∎

PROPOSITION 29. *Let* $m \geq 2$ *and let* $\boldsymbol{a} = (a_1, \dots, a_n) \in \mathbb{Z}^n$. *If the extension* $\mathbb{Q}(\zeta_m, \sqrt[m]{\boldsymbol{a}})/\mathbb{Q}(\zeta_m)$ *is tamely ramified, then its Steinitz class is trivial.*

Proof. By Proposition 13, if the extension $\mathbb{Q}(\zeta_m, \sqrt[m]{\boldsymbol{a}})/\mathbb{Q}(\zeta_m)$ is tamely ramified, then its Steinitz class is $(\prod_{\boldsymbol{r} \in \hat{\mathcal{R}}} \mathcal{B}_{\boldsymbol{r}})^{-1}$, where the $\mathcal{B}_{\boldsymbol{r}}$'s are the ideals associated to $\boldsymbol{a}$, and these ideals are principal by Corollary 28. ∎

A similar result for cyclic Kummer extension of degree p^n generated by roots of rational integers, not necessarily tame, can be found in [2].

3.3. Normal integral bases. Recently Ichimura [8], generalising Kawamoto's result [10] on cyclic extensions of prime degree, showed that tame ramification is a sufficient condition for the existence of a NIB for any cyclic extension $\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}(\zeta_m)$ with m square-free and $(a, m) = 1$. Below, we give a different proof of Ichimura's result, based on our Theorem 11. Moreover, we consider the question whether for the more general case of extensions $\mathbb{Q}(\zeta_m, \sqrt[m]{\boldsymbol{a}})/\mathbb{Q}(\zeta_m)$ with m square-free and $(a_i, m) = 1$ for all i, tame ramification is still a sufficient condition for the existence of a NIB. We show that the answer is negative in general (see Example 1); moreover, in Proposition 35 we collect some cases with positive answer.

LEMMA 30. *Let* $m \geq 2$ *be a positive square-free integer. For any integer* $a \in \mathbb{Z}$ *with* $(a, m) = 1$, *there exists a unit* $u \in \mathbb{Z}[\zeta_m]^*$ *such that* $u \equiv a \pmod{m}$.

Proof. This is a special case of the general principal ideal theorem given by Miyake [13, Thm. 1]. ∎

PROPOSITION 31 (Kawamoto's Theorem). *Let p be an odd prime number and let $a \in \mathbb{Z}$ be such that $a^{p-1} \equiv 1 \pmod{p^2}$. Then $\mathbb{Q}(\zeta_p, \sqrt[p]{a})/\mathbb{Q}(\zeta_p)$ has a NIB.*

Proof. For the case when a is p-power free see [10]. If $a = b^p \cdot \tilde{a}$, then $\mathbb{Q}(\zeta_p, \sqrt[p]{a}) = \mathbb{Q}(\zeta_p, \sqrt[p]{\tilde{a}})$ and

$$a^{p-1} = b^{p(p-1)}\tilde{a}^{p-1} \equiv \tilde{a}^{p-1} \pmod{p^2},$$

thus the proposition easily follows. ∎

REMARK 32. Thanks to Corollary 25, the previous result tells that $\mathbb{Q}(\zeta_p, \sqrt[p]{a})/\mathbb{Q}(\zeta_p)$ has a NIB whenever it is tamely ramified (as already pointed out by Kawamoto).

PROPOSITION 33. *Let $m \geq 2$ be a positive square-free integer and let $a \in \mathbb{Z}$ be such that $(a, m) = 1$. Then the extension $\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}(\zeta_m)$ has a NIB whenever it is tame.*

We remark that this result is contained in [8]; we give a different proof, based on our Theorem 11.

Proof. We set $L = \mathbb{Q}(\zeta_m, \sqrt[m]{a})$ and $K = \mathbb{Q}(\zeta_m)$.

Let $m = p_1 \cdots p_k$, with p_i pairwise distinct prime numbers, and (possibly rearranging the indices) let $\{p_1, \dots p_n\}$ be the primes dividing m such that $\sqrt[p_i]{a} \notin K$.

We define

$$\boldsymbol{a} = \{a_1 \dots, a_n\} := \{a^{m/p_1}, \dots, a^{m/p_n}\},$$
$$\boldsymbol{\alpha} = \{\alpha_1, \dots, \alpha_n\} := \sqrt[m]{\boldsymbol{a}} = \{\sqrt[p_1]{a}, \dots, \sqrt[p_n]{a}\}.$$

Thus we have

$$L = K(\sqrt[m]{a}) = K(\sqrt[p_1]{a}, \dots, \sqrt[p_n]{a}) = K(\alpha_1, \dots, \alpha_n) = K(\sqrt[m]{\boldsymbol{a}}).$$

By Kawamoto's Theorem, for $1 \leq i \leq n$, there exists a NIB ω_i of the extension $\mathbb{Q}(\zeta_{p_i}, \alpha_i)/\mathbb{Q}(\zeta_{p_i})$. This NIB translates to $K(\alpha_i)/K$: in fact, K and $\mathbb{Q}(\zeta_{p_i}, \alpha_i)$ are linearly disjoint over $\mathbb{Q}(\zeta_{p_i})$, since a is coprime to m.

For each $i = 1, \dots, n$, consider the ideals $\mathcal{B}_{i,r}$ associated to a_i; by Corollary 28 these ideals are generated by rational integers $b_{i,r}$, and by Theorem 11 (case $n = 1$) we have

$$p_i\omega_i = \sum_{r=0}^{p_i-1} u_{i,r}\frac{\alpha_i^r}{b_{i,r}},$$

with $u_{i,r} \in \mathbb{Z}[\zeta_{p_i}]^* \subset \mathbb{Z}[\zeta_m]^*$. Then

$$\prod_{i=1}^{n}\Big(\sum_{r=0}^{p_i-1} u_{i,r}\frac{\alpha_i^r}{b_{i,r}}\Big) = \prod_{i=1}^{n} p_i\omega_i = m\prod_{i=1}^{n}\omega_i \equiv 0 \pmod m,$$

or equivalently, letting $\hat{\mathcal{R}}$ be as in Section 2,

$$\sum_{\boldsymbol{r}\in\hat{\mathcal{R}}} \boldsymbol{\alpha}^{\boldsymbol{r}} \prod_{i=1}^{n} \frac{u_{i,r_i}}{b_{i,r_i}} \equiv 0 \pmod m.$$

By Lemma 30 we know that $b_{i,r_i} \equiv v_{i,r_i} \pmod m$ with $v_{i,r_i} \in \mathbb{Z}[\zeta_m]^*$; setting $\varepsilon_{\boldsymbol{r}} = \prod_{i=1}^{n}(u_{i,r_i}/v_{i,r_i}) \in \mathbb{Z}[\zeta_m]^*$ we get

$$\sum_{\boldsymbol{r}\in\hat{\mathcal{R}}} \varepsilon_{\boldsymbol{r}}\boldsymbol{\alpha}^{\boldsymbol{r}} \equiv 0 \pmod m. \tag{5}$$

For each $r \in \hat{\mathcal{R}}$, let $b_{\boldsymbol{r}}$ be the rational integer given by Corollary 28 which generates the ideal $\mathcal{B}_{\boldsymbol{r}}$ associated to $\boldsymbol{a}$; it is clear that condition (i) of Theorem 11 is satisfied by $\boldsymbol{a}$. Let us show that also condition (ii) is satisfied, so that we get a NIB for the extension we are considering.

For each $\boldsymbol{r} \in \hat{\mathcal{R}}$, we are looking for units $u_{\boldsymbol{r}}$ such that

$$\sum_{\boldsymbol{r}\in\hat{\mathcal{R}}} u_{\boldsymbol{r}}\frac{\boldsymbol{\alpha}^{\boldsymbol{r}}}{b_{\boldsymbol{r}}} \equiv 0 \pmod m.$$

By Lemma 30, we know that $b_{\boldsymbol{r}} \equiv v_{\boldsymbol{r}} \pmod m$ with $v_{\boldsymbol{r}} \in \mathbb{Z}[\zeta_m]^*$; setting $u_{\boldsymbol{r}} = \varepsilon_{\boldsymbol{r}} v_{\boldsymbol{r}}$ we get

$$\sum_{\boldsymbol{r}\in\hat{\mathcal{R}}} u_{\boldsymbol{r}}\frac{\boldsymbol{\alpha}^{\boldsymbol{r}}}{b_{\boldsymbol{r}}} = \sum_{\boldsymbol{r}\in\hat{\mathcal{R}}} \varepsilon_{\boldsymbol{r}} v_{\boldsymbol{r}}\frac{\boldsymbol{\alpha}^{\boldsymbol{r}}}{b_{\boldsymbol{r}}} \equiv \sum_{\boldsymbol{r}\in\hat{\mathcal{R}}} \varepsilon_{\boldsymbol{r}}\boldsymbol{\alpha}^{\boldsymbol{r}} \equiv 0 \pmod m,$$

where the last congruence is due to (5). ∎

Corollary 34. *Let $m \geq 2$ be a positive square-free integer and let $m = p_1 \cdots p_r$ be its factorization into prime factors. Let $a \in \mathbb{Z}$ be such that $(a, m) = 1$. Then the extension $\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}(\zeta_m)$ has a NIB if and only if*

$$a^{p_i-1} \equiv 1 \pmod{p_i^2} \quad \text{for all } i = 1, \ldots, r.$$

Proof. This follows from Proposition 33 and Corollary 25. ∎

Consider now the case of an abelian extension $\mathbb{Q}(\zeta_m, \sqrt[m]{\boldsymbol{a}})/\mathbb{Q}(\zeta_m)$ generated by mth roots of n integers $a_1, \ldots, a_n$ coprime to m where m is a square-free integer. Also in this case, the tameness condition can be made completely explicit; in fact, the extension $\mathbb{Q}(\zeta_m, \sqrt[m]{a_1}, \ldots, \sqrt[m]{a_n})/\mathbb{Q}(\zeta_m)$ is tamely ramified if and only if its subextensions $\mathbb{Q}(\zeta_m, \sqrt[m]{a_i})/\mathbb{Q}(\zeta_m)$ are tamely ramified for all $i = 1, \ldots, n$, hence if and only if a_i satisfies the conditions of Corollary 34 for all i.

We can ask whether the result of Proposition 33 can be generalised to this case, namely if the tameness of the extension is sufficient to ensure the existence of a NIB.

The following example shows that, in general, the answer is negative.

EXAMPLE 1. $\mathbb{Q}(\zeta_3, \sqrt[3]{10}, \sqrt[3]{46})/\mathbb{Q}(\zeta_3)$ is tamely ramified but has no normal integral basis.

Proof. Let $K = \mathbb{Q}(\zeta_3)$, and let $L = K(\sqrt[3]{10}, \sqrt[3]{46})$; since $10 \equiv 1 \pmod 9$, and $46 \equiv 1 \pmod 9$ the extension L/K is tamely ramified.

Let α be any root of $x^3 - 10$ and let β be any root $x^3 - 46$. With the notation of Theorem 11, L/K has a normal integral basis if and only if there exist units $u_{ij} \in \mathcal{O}_K^*$ such that the element

$$\omega = \frac{1}{9}\Bigg(1 + u_{10}\alpha + u_{20}\alpha^2 + u_{01}\beta + u_{02}\beta^2 + u_{11}\alpha\beta + \frac{u_{21}}{2}\alpha^2\beta + \frac{u_{12}}{2}\alpha\beta^2 + \frac{u_{22}}{2}\alpha^2\beta^2\Bigg)$$

is an integer. We want to show that this is not the case.

Since $\mathcal{O}_K^* = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$, the computation can be easily performed by a computer program. Anyway, to make it clear to the reader, we sketch an easy pen-and-paper proof.

First, we note that if $u, v \in \mathcal{O}_K^*$ and $\gamma \in \{\alpha, \beta, \alpha\beta, \alpha^2\beta\}$ then

$$1 + u\gamma + v\gamma^2 \equiv 0 \pmod 3 \;\Leftrightarrow\; (u, v) \in \{(1,1); (\zeta_3, \zeta_3^2); (\zeta_3^2, \zeta_3)\} \tag{6}$$

(For $\Leftarrow$ see [7, Lemma 7]; and $\Rightarrow$ is easily seen by explicit computation.)

The idea now is to use the integrality of the traces of integral elements over intermediate fields to get a restriction on the u_{ij}.

- $\mathrm{tr}_{L/K(\alpha)}(\omega) = \frac{1}{3}(1 + u_{10}\alpha + u_{20}\alpha^2)$; as this element is an integer, we must have
$$1 + u_{10}\alpha + u_{20}\alpha^2 \equiv 0 \pmod 3.$$
Using (6) and possibly replacing α with one of it conjugates we can assume $u_{10} = 1$, hence $u_{20} = 1$.
- $\mathrm{tr}_{L/K(\beta)}(\omega)$ integral $\Rightarrow 1 + u_{01}\beta + u_{02}\beta^2 \equiv 0 \pmod 3$: we may choose β such that $u_{01} = 1$, then $u_{02} = 1$.
- $\mathrm{tr}_{L/K(\alpha\beta)}(\omega)$ integral $\Rightarrow 1 + u_{11}\alpha\beta - u_{22}\alpha^2\beta^2 \equiv 0 \pmod 3$: this, according to (6), gives two cases:
  (A) $u_{11} = 1$, hence $u_{22} = -1$,
  (B) $u_{11} = \zeta_3$, hence $u_{22} = -\zeta_3^2$;
  the case $u_{11} = \zeta_3^2$ is identical to case (B).
- $\mathrm{tr}_{L/K(\alpha)}(\beta^2\omega)$ integral $\Rightarrow u_{01} + u_{11}\alpha - u_{21}\alpha^2 \equiv 0 \pmod 3$,
  $\mathrm{tr}_{L/K(\beta)}(\alpha^2\omega)$ integral $\Rightarrow u_{10} + u_{11}\beta - u_{12}\beta^2 \equiv 0 \pmod 3$:

(A) $u_{21} = u_{12} = -1$,
(B) $u_{21} = u_{12} = -\zeta_3^2$.

- $\mathrm{tr}_{L/K(\alpha^2\beta)}(\omega)$ integral $\Rightarrow 1 - u_{12}\alpha\beta^2 - u_{21}\alpha^2\beta^2 \equiv 0 \pmod 3$: case (B) gives a contradiction with (6), whereas case (A) is possible.

It remains to test the single element

$$\omega = \tfrac{1}{9}\big(1 + \alpha + \alpha^2 + \beta + \beta^2 + \alpha\beta - \tfrac{1}{2}\alpha^2\beta - \tfrac{1}{2}\alpha\beta^2 - \tfrac{1}{2}\alpha^2\beta^2\big);$$

we can now compute the norm of ω over K, which is $-1604800/9$, so ω is not an integer. ∎

PROPOSITION 35. *Let $m \geq 2$ be a positive square-free integer and $\boldsymbol{a} \in \mathbb{Z}^n$ such that $(a_i, m) = 1$ for all i. Moreover, assume that $(a_i, a_j) = 1$ for all $i \neq j$. Then the extension $\mathbb{Q}(\zeta_m, \sqrt[m]{\boldsymbol{a}})/\mathbb{Q}(\zeta_m)$ has a NIB whenever it is tame.*

Proof. The first step is to show that, up to replacing the elements a_i with $a_i^{d_i}$ for suitable $d_i \mid m$, we may suppose that the extensions $\mathbb{Q}(\zeta_m, \sqrt[m]{a_i})$ are all linearly disjoint over $\mathbb{Q}(\zeta_m)$, namely that, if we put $N = [\mathbb{Q}(\zeta_m, \sqrt[m]{\boldsymbol{a}}) : \mathbb{Q}(\zeta_m)]$ and $m_i = [\mathbb{Q}(\zeta_m, \sqrt[m]{a_i}) : \mathbb{Q}(\zeta_m)]$, then $N = \prod_i m_i$. In fact, we observe that we can reduce to the case when m is a prime, since if $m = p_1 \cdots p_r$, then $\mathbb{Q}(\zeta_m, \sqrt[m]{\boldsymbol{a}})$ is the compositum of the extensions $\mathbb{Q}(\zeta_m, \sqrt[p_j]{\boldsymbol{a}})$ for $j = 1, \ldots, r$ which are clearly linearly disjoint over $\mathbb{Q}(\zeta_m)$. In the case when $m = p$ is a prime it is easy to see that, if $[\mathbb{Q}(\zeta_p, \sqrt[p]{\boldsymbol{a}}) : \mathbb{Q}(\zeta_p)] = p^{n-k}$, we can omit k of the n generators $\{\sqrt[p]{a_1}, \ldots, \sqrt[p]{a_n}\}$. We also note that this substitution does not affect the conditions $(a_i, a_j) = 1$.

We now note that, thanks to the previous proposition, for any i the extension $\mathbb{Q}(\zeta_m, \sqrt[m]{a_i})/\mathbb{Q}(\zeta_m)$ has a NIB ω_i.

Since the extensions $\mathbb{Q}(\zeta_m, \sqrt[m]{a_i})/\mathbb{Q}(\zeta_m)$ are linearly disjoint, it follows that $\omega = \prod_{i=1}^n \omega_i$ generates a normal integral basis for $\mathbb{Q}(\zeta_m, \sqrt[m]{\boldsymbol{a}})/\mathbb{Q}(\zeta_m)$. ∎

REMARK 36. We note that each extension $L = \mathbb{Q}(\zeta_m, \sqrt[m]{\boldsymbol{a}})$ can be embedded in a Kummer extension $E = \mathbb{Q}(\zeta_m, \sqrt[m]{a_1'}, \ldots \sqrt[m]{a_t'})$ with $(a_i', a_j') = 1$ for all $i \neq j$: for example, this can be obtained by choosing as generators the mth roots of all primes dividing $\prod_i a_i$ (in a concrete case one can often find a smaller extension with the same property).

In the case when the extension E/K is tame, the extension L/K has a normal integral basis: in fact, E/K has a NIB ω by Proposition 35, hence $\mathrm{tr}_{E/L}(\omega)$ is a generator for a normal integral basis of L/K.

However, the extension E/K obtained from L might no longer be tame.

3.4. A special case. In this last section we recall a result by Ichimura showing that, under particular hypotheses on m and a, a generator of a NIB of $\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}(\zeta_m)$ can be explicitly given, and we verify moreover that this explicit element, multiplied by ζ_m, generates a NIB of $\mathbb{Q}(\zeta_m, \sqrt[m]{a})$ over $\mathbb{Q}$.

PROPOSITION 37. *Let m be a positive integer, set $\tilde{m} = m\prod_{p|m} p$ and let $a \in \mathbb{Z}$ be a square-free integer such that $a \equiv 1 \pmod{\tilde{m}}$. Then*

$$\omega = \frac{1}{m}\sum_{i=0}^{m-1} \sqrt[m]{a}^{\,i}$$

is a NIB generator for the extension $\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}(\zeta_m)$.

Proof. See [7, Corollary 3]. The explicit generator can be found in the proof. ∎

PROPOSITION 38. *Let $m \geq 2$ and a be square-free integers such that $a \equiv 1 \pmod{m^2}$ and let ω be the NIB of the extension $\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}(\zeta_m)$ given in Proposition 37. Then $\omega\zeta_m$ is a NIB for the non-abelian extension $\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}$.*

Proof. Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q})$, and $H = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. For any $h \in H$ there exists $g \in G$ such that $g|_{\mathbb{Q}(\zeta_m)} = h$ and $g(\sqrt[m]{a}) = \sqrt[m]{a}$, denote this g by g_h. We also denote by $\bar{g} \in G$ the generator of the cyclic subgroup $\mathrm{Gal}(\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}(\zeta_m))$ such that $\bar{g}(\sqrt[m]{a}) = \zeta_m \sqrt[m]{a}$. Then

$$G = \{\bar{g}^i g_h \mid 0 \leq i \leq m-1,\, h \in H\}.$$

Setting $L = \mathbb{Q}(\zeta_m, \sqrt[m]{a})$ and $K = \mathbb{Q}(\zeta_m)$, from Proposition 37 we have

$$\mathcal{O}_L = \bigoplus_{i=0}^{m-1} \mathcal{O}_K \bar{g}^i(\omega). \tag{7}$$

It is well known that

$$\mathcal{O}_K = \bigoplus_{h\in H} \mathbb{Z}h(\zeta_m). \tag{8}$$

Equations (7) and (8) together give

$$\mathcal{O}_L = \bigoplus_{i=0}^{m-1}\bigoplus_{h\in H} \mathbb{Z}\bar{g}^i(\omega)h(\zeta_m).$$

But $\bar{g}^i(\omega)h(\zeta_m) = \bar{g}^i g_h(\omega\zeta_m)$, i.e. $\mathcal{O}_L = \mathbb{Z}[G]\omega\zeta_m$. ∎

Acknowledgements. We would like to thank Professors Nigel Byott and Cornelius Greither for their careful reading of our paper and for their suggestions.

References

[1] W. A. Adkins and S. H. Weintraub, *Algebra. An Approach via Module Theory*, Grad. Texts in Math. 136, Springer, 1992.

[2] L. Caputo and V. Di Proietto, *Steinitz classes and integral bases of radical extensions of number fields*, in preparation.

[3] I. Del Corso and L. P. Rossi, *Normal integral bases for cyclic Kummer extensions*, J. Pure Appl. Algebra 214 (2010), 385–391.
[4] A. Fröhlich, *Arithmetic and Galois module structure for tame extensions*, J. Reine Angew. Math. 286–287 (1976), 380–440.
[5] E. J. Gómez Ayala, *Bases normales d'entiers dans les extensions de Kummer de degré premier*, J. Théor. Nombres Bordeaux 6 (1994), 95–116.
[6] C. Greither, D. Replogle, K. Rubin and A. Srivastav, *Swan modules and Hilbert–Speiser number fields*, J. Number Theory 79 (1999), 164–173.
[7] H. Ichimura, *On the ring of integers of a tame Kummer extension over a number field*, J. Pure Appl. Algebra 187 (2004), 169–182.
[8] H. Ichimura, *On the integer ring of a Kummer extension generated by a power root of a rational number*, Yokohama Math. J. 55 (2010), 165–170.
[9] J. W. Jones and D. P. Roberts, *Database of Local Fields*, http://math.asu.edu/jj/localfields/.
[10] F. Kawamoto, *Remark on "On normal integral bases"*, Tokyo J. Math. 8 (1985), 275.
[11] S. Lang, *Algebraic Number Theory*, Grad. Texts in Math. 110, Springer, 1986.
[12] S. Lang, *Algebra*, 3rd ed., Grad. Texts in Math. 211, Springer, 2002.
[13] K. Miyake, *On the general principal ideal theorem*, Proc. Japan Acad. 56A (1980), 171–174.
[14] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., Springer, 2004.

Ilaria Del Corso
Dipartimento di Matematica
Università di Pisa
Largo B. Pontecorvo, 5
56127 Pisa, Italy
E-mail: delcorso@dm.unipi.it

Lorenzo Paolo Rossi
Scuola Normale Superiore
Piazza dei Cavalieri, 7
56126 Pisa, Italy
E-mail: l.rossi@sns.it

Received on 25.6.2012
and in revised form on 25.1.2013 (7111)